



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
08/927,382	09/12/1997	MICHAEL JOHN COSS	1-1-1	8320

7590

12/21/2004

JOSEPH B RYAN  
RYAN AND MASON, L.L.P.  
90 FOREST AVENUE  
LOCUST VALLEY, NY 11560

EXAMINER
----------

REVAK, CHRISTOPHER A

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 12/21/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

08/927,382

Applicant(s)

COSS ET AL.

Examiner

Christopher A. Revak

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 07 September 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-26 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-26 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |   |   |
|---|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)                        | 4) <input type="checkbox"/> Interview Summary (PTO-413)                     |
| 2) <input type="checkbox"/> Notice of Draftperson's Patent Drawing Review (PTO-948)     | Paper No(s)/Mail Date. _____  |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date. _____  | 6) <input type="checkbox"/> Other: _____                                    |

## **DETAILED ACTION**

### ***Response to Arguments***

1. Applicant's arguments filed September 7, 2004 have been fully considered but they are not persuasive. The examiner is interpreting the term "security policy" as that is a collection of rules that dictate how the security policy is to be enforced. The instant application discloses, "The security policies can be represented by sets of access rules" as is recited on page 5, line 23 of the applicant's specification. The Examiner's interpretation is consistent with that of the applicant's. To further support the examiner's interpretation, in a reference submitted as IDS by the applicant, Amoroso et al discloses that "a security policy consists the access control requirements specification for the information and other assets within an organization" as is recited on page 144. The The examiner contends that this interpretation of "security policies containing a collection of rules" is consistent with that of the prior art and the applicant and is adequate to meet the applicant's claim language of a plurality of rules since the security policy contains multiple, or a plurality, of rules as is disclosed by Shwed.

It is additionally argued by the applicant that a plurality of administrators are associated with a plurality of domains. The examiner respectfully disagrees and it is interpreted by the examiner that there exists multiple administrators for a plurality of domains since it is disclosed by Shwed '726 et al that there can exist a number of network configurations can be virtually limitless, namely configuring a plurality of

domains with a plurality of administrators (col. 5, lines 39-54). Shwed '668 discloses the some recitations as per column 3, lines 27-43.

2. The examiner has hereby withdrawn the rejection of claims 3-5 under 35 U.S.C. 112 second paragraph.

***Claim Rejections - 35 USC § 102***

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-26 are rejected under 35 U.S.C. 102(e) as being anticipated by Shwed et al, U.S. Patent 5,835,726.

As per claims 1,8,12,17, and 22, it is taught by Shwed et al of a method and computer system for validating packets in a computer network by means of a firewall (col. 2, lines 26-29,41-44, col. 3, lines 42-45, and col. 14, lines 62-65). It is inherent that a processor is contained within the teachings of Shwed et al since processors are important for being the control unit of a computer for fetching and executing instructions to perform specific tasks. A client initiates a request for a session with a host (col. 20, line 65 through col. 21, line 2). A session key is agreed upon (by deriving it) in regards to the packets/data items (col. 15, lines 28-30). A rule base (containing a security

policy) is maintained (by pre-selecting) as to handling inbound and outbound communications packets that includes function of a session key (col. 14, line 59 through col. 15, line 2). The security policy is comprised of multiple security rules that dictate if the packet is to be accepted (validated) or denied based on the filtering language instructions (col. 2, lines 45-50, col. 4, lines 1-6, and col. 6, lines 35-38). It is interpreted by the examiner that there exists multiple, independent, security policies since it is disclosed by Shwed et al that there exists different departments and individuals with varying titles at an organization (col. 6, line 62 through col. 7, line 11).

As per claim 2, Shwed et al discloses of a session key associated with header information associated (appended) with the packet (col. 17, lines 60-64).

As per claim 3, it is taught by Shwed et al of the session key is included with the source and destination addresses (col. 17, lines 44-52).

As per claim 4, it is disclosed by Shwed et al of the session key is included with the source and destination IP addresses (col. 17, lines 44-52).

As per claim 5, Shwed et al discloses of the use of transmission control protocol (TCP) for the type (next level) of protocol (col. 18, lines 1-3).

As per claims 6,18,19,23, and 24, it is recited in the teachings of Shwed et al of a plurality of network interfaces located in each computer on the network (col. 9, lines 6-8). The source IP address indicates where a request was sent from, i.e. the sending network interface (col. 20, lines 2-4).

As per claims 7,20,21,25, and 26, it is taught by Shwed et al of a plurality of network interfaces located in each computer on the network (col. 9, lines 6-8). The

destination (where the request is to be sent) IP address indicates where a request is sent to, i.e. the destination network interface (col. 22, lines 50-52).

As per claims 9,10,13, and 14, Shwed et al discloses of a security policy comprises of multiple security rules that dictate if the packet is to be accepted (validated) or denied based on the filtering language instructions as is based on a firewall (col. 2, lines 45-50, col. 4, lines 1-6, col. 6, lines 35-38, and col. 14, lines 62-65). It is based on different groups and subgroups within a given group (col. 6, line 62 through col. 7, line 11 and as shown in Figure 3-2).

As per claims 11 and 15, it is taught by Shwed et al of an administrator for a given group has the ability to modify the rules of a security policy for a group (col. 3, lines 39-54, col. 6, line 62 through col. 7, line 11, col. 7, lines 61-65, and as shown in Figure 3-2).

As per claim 16, Shwed et al discloses of a method and computer system for validating packets in a computer network by means of a firewall (col. 2, lines 26-29,41-44, and col. 14, lines 62-65). A session key is agreed upon (by deriving it) in regards to the packets (col. 15, lines 28-30). A rule base (containing a security policy) is maintained as to handling inbound and outbound communications packets that includes function of a session key (col. 14, line 59 through col. 15, line 2). The security policy is comprised of multiple security rules that dictate if the packet is to be accepted (validated) or denied based on the filtering language instructions (col. 2, lines 45-50, col. 4, lines 1-6, and col. 6, lines 35-38). It is shown in Figure 3-2 of a plurality of domains that have multiple security policies applied to (col. 6, lines 35-38). An administrator for a

Art Unit: 2131

given group has the ability to modify the rules of a security policy for a group (col. 3, lines 39-54, col. 6, line 62 through col. 7, line 11, col. 7, lines 61-65, and as shown in Figure 3-2). It is interpreted by the examiner that there exists multiple administrators for a plurality of domains since it is disclosed by Shwed et al that there can exist a number of network configurations can be virtually limitless, namely configuring a plurality of domains with a plurality of administrators (col. 5, lines 39-54).

***Claim Rejections - 35 USC § 103***

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 1-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shwed, U.S. Patent 5,606,668.

As per claims 1-7, 17-21, and 22-26, Shwed describes a security system for a computer network that implements packet filtering (col. 3, lines 59-65). Shwed teaches that his system applies a particular security rule to an incoming packet (col. 7, lines 14-24) based on data extracted from the incoming packet (col. 8 lines 39-49 and Fig 8). The security policy is comprised of multiple security rules that dictate if the packet is to be accepted (validated) or denied based on the filtering language instructions (col. 2, lines 1-4, 45-54 and col. 4, lines 23-26).

As per claim 1, Shwed does not explicitly teach that his system derives a session key for the incoming packet. However, processing the extracted packet data in the Shwed invention (col. 8, line 39 to col. 9, line 63) would have been recognized by one of ordinary skill in the art, at the time the invention was made, as an obvious equivalent to deriving a session key for the incoming packet, because a session key indicates which security rule to use for a particular packet. Shwed further teaches that a specific TCP destination port may be among the data extracted from the incoming packet (col. 9, line 64 to col. 10, line 14). Shwed further teaches that his system is implemented using gateways having multiple network interfaces (Fig 2), where the gateway is connected through a router to the Internet.

As per claims 2,3,4,5,19,21,24, and 26, Shwed does not explicitly teach that his invention processes all types of Internet protocol packets, such as UDP packets, or all useful packet data, such as IP addresses. However, the Internet was well-known to those of ordinary skill in the art, at the time the invention was made, to utilize layered communication protocols, including UDP in addition to TCP, and it was also well-known to those skilled in the art that methods used to extract data from the headers of TCP packets could be utilized to extract data from UDP packets as well, and that these methods could have been utilized to extract many types of packet header information, including source address, destination address, next-level protocol, source port, and destination port data. It would have been obvious to one skilled in the art, at the time the invention was made, to program the Shwed invention to process all types of Internet protocol packets and to extract all useful packet header data to assist in security rule



decision making, because this would have been easy to accomplish within the Shwed system and would enable the Shwed system to meet a wide range of user security requirements.

As per claims 6,7,18,20,23, and 25, Shwed teaches that his system is implemented using gateways having multiple network interfaces (Fig 2), where the gateway is connected through a router to the Internet. Gateways were well-known to those of ordinary skill in the art, at the time the invention was made, to allow packets to be routed to different network interfaces based on well-known routing algorithms, and that these routing algorithms could be simply and favorably utilized in conjunction with network security algorithms like those taught by Shwed (col. 8 lines 39-49 and Fig 8).

As per claims 8-11,12-15, and 16, Shwed describes a security system for a computer network that implements packet filtering (col. 3, lines 59-65). Shwed teaches that his system applies a particular security rule to an incoming packet (col. 7, lines 14-24) based on data extracted from the incoming packet (col. 8, lines 39-49, and Fig 8). The security policy is comprised of multiple security rules that dictate if the packet is to be accepted (validated) or denied based on the filtering language instructions (col. 2, lines 1-4,45-54 and col. 4, lines 23-26). It is shown in Figure 3-2 of a plurality of domains that have multiple security policies applied to (col. 4, lines 23-26). An administrator for a given group has the ability to modify the rules of a security policy for a group (col. 4, lines 39-42,60-65, col. 5, lines 51-56, and as shown in Figure 3-2). It is interpreted by the examiner that there exists multiple administrators for a plurality of domains since it is disclosed by Shwed et al that there can exist a number of network

configurations can be virtually limitless, namely configuring a plurality of domains with a plurality of administrators (col. 3, lines 27-43).

As per claims 8,9,10,12,13, and 14, Shwed does not explicitly teach the use of multiple independent security policies, administered by separate administrators and applied to different groups. However, Shwed further teaches (col. 4, lines 27-67) that a system administrator may create security rules, and may designate that network objects be separated into sub-groups or domains, where sub-groups may utilize different sets of security rules (column 4, lines 23-26 and lines 50-57) which would implement multiple sets of security policies. (Shwed uses as an example a communication group composed of a company's CEO, CFO, directors; security rules could be set up in the Shwed system to allow direct communication by this group, but not others, to a finance group (col. 4, lines 59-63)). It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to allow the creation of specific security rules for a particular sub-group of network objects, because this could be accomplished with little modification to the Shwed system, and because the creation of independent security policies by the creation of multiple sets of rules would give users of the Shwed system the benefits of hierarchies of security.

As per claims 11,15, and 16, although Shwed does not explicitly teach that only the administrator of a domain is allowed to modify the security policy rules for that domain, it would have been obvious to one of ordinary skill in the art, at the time, the invention was made, to restrict the creation of security rules for a particular sub-group of network objects to a particular system administrator, because this could be

accomplished with little, if any, modification to the Shwed system, and because the creation of rules by a specialist in a particular domain would give the benefits of increased security and confidence in the Shwed system.

### ***Conclusion***

7. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 703-305-1843. The examiner can normally be reached on Monday-Friday, 6:30am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

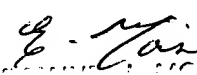
Art Unit: 2131

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christopher Revak  
AU 2131

CR

  
December 16, 2004

  
CHRISTOPHER REVAK  
PATENT ATTORNEY